

REMARKS

Claims 1-34 are pending. Claims 1, 3, 10-12 and 19-20 are amended, and claims 2 and 33 are cancelled with this response. Reconsideration of the application is respectfully requested based on the following remarks.

I. OBJECTION TO THE SPECIFICATION

The specification was objected to because the application numbers on page 1 need to be updated. The specification has been amended to address this issue. Accordingly, withdrawal of the objection is respectfully requested.

II. REJECTION OF CLAIMS 1-34 UNDER 35 U.S.C. § 102(e)

Claims 1-34 were rejected under 35 U.S.C. § 102(e), as being anticipated by U.S. Patent No. 7,142,671 (Qi et al.). Withdrawal of the rejection is respectfully requested for at least the following reasons.

- i. Qi et al. do not teach a security processing circuit having a DES engine that comprises a data input multiplexer, an intermediate result register, and eight cipher blocks, as recited in claims 1 and 19.*

Claims 1 and 19 are directed to a security processing circuit that comprises a DES engine. The DES engine comprises a data input multiplexer that is operable to select and couple one of two inputs to an output thereof, and an intermediate result register that is operable to store right and left half results of an initial permutation or of an eight round cipher process performed by eight cipher blocks, based on data present at a data input thereof.

Qi et al. do teach multiplexers at 409 and do teach registers at 411, 413, however, ***any cipher process results are not that of an eight round cipher process as claimed.*** Rather, the processing between 411, 413 and 431 prior to the feedback is a full sixteen (16) rounds. (See, e.g., Col. 7, lines 18-29). Therefore Qi et al. do not teach this feature and thus does not anticipate the invention of claim 1.

- ii. Qi et al. do not teach the cipher output of the eight cipher blocks feedback coupled to the data input multiplexer and to an input of a pre-data output multiplexer, as recited in claims 1 and 19.**

The DES engine of claims 1 and 19 further comprises eight cipher blocks operable to output first and second results of a sequential eight step cipher process **during a first and second eight step cycle of each of the three DES processing operations.** The cipher output is feedback coupled to the data input multiplexer and to an input of a pre-data output multiplexer to facilitate the 3DES processing. Qi et al. do not teach this feature.

Initially, Qi et al. do not teach eight cipher blocks as claimed. Rather, as shown in Figs. 4A, 4B and 5, and in corresponds text of columns 7 and 8, sixteen (16) rounds are performed corresponding to a full DES round before any feedback. In addition, no pre-data output multiplexer to receive the cipher results is provided as claimed. Therefore Qi et al. do not anticipate the invention of claim 1.

- iii. Qi et al. do not teach cipher processing a stored permutation using eight cipher blocks, storing it as an intermediate result, and cipher processing the stored intermediate result using the eight cipher blocks, as recited in claims 27, 30 and 34.**

Claims 27, 30 and 34 are directed to method of performing security processing, comprising cipher processing a stored permutation result using eight cipher blocks to generate an intermediate result, selectively storing the intermediate result, and cipher processing the intermediate result using the eight cipher blocks to thereby generate a first DES result.

Qi et al. do not teach this feature. Rather, as cited above, Qi et al. perform a traditional sixteen (16) rounds of cipher processing prior to any feedback, and thus do not perform two passes of cipher processing using eight cipher blocks to generate a

first DES result as claimed. Therefore Qi et al. do not anticipate the invention of claims 27, 30 and 34. Accordingly, withdrawal of the rejection is respectfully requested.

III. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be in condition for allowance.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should any fees be due as a result of the filing of this response, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, AMDP782US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

By /Thomas G. Eschweiler/
Thomas G. Eschweiler
Reg. No. 36,981

National City Bank Building
629 Euclid Avenue, Suite 1000
Cleveland, Ohio 44114
(216) 502-0600